

COLONEL JOHN W. HAYDEN JR., POLICE COMMISSIONER

Service, Integrity, Leadership And Fair Treatment To All

METROPOLITAN POLICE DEPARTMENT

CITY OF ST. LOUIS – 1915 Olive Street - ST. LOUIS, MISSOURI 63103

August 22, 2019

MuckRock News
Attn: Freddy Martinez
DEPT MR 76450
411A Highland Avenue
Somerville, MA 02144-2516

RE: Records and materials related to the solicitation, acquisition, and use of face recognition technology and related software and services.

Dear Ms. Martinez:

Please see below response to your Sunshine request regarding face recognition technology and related software and services:

- Agreements: Contracts (including non-disclosure agreements), licensing agreements, nondisclosure agreements. – **See enclosed MOU-SMRT Project**
- Bid records: Requests For Proposal (or equivalent calls for bids), sole source or limited source justification and approval documentation, documentation of selection, and other materials generated in the consideration and selection of the technology in question – **No responsive records.**
- Company relations and communications: records related to meetings or follow-up actions with any vendors, companies, or other private entities marketing face recognition to this agency for immigration, intelligence, law enforcement, or other use. – **Please clarify search terms you would like to use in order to conduct an email search from January 1, 2017-present. Be advised a cost estimate will be provided prior to performing the search.**
- Financial records: purchase orders, invoices, and other memoranda and documentation. – **No responsive records.**
- Marketing records: All marketing materials – unsolicited, requested, or otherwise – acquired from vendors of face recognition technology – **Please clarify search terms you would like to use in order to conduct an email search from January 1, 2017-present. Be advised a cost estimate will be provided prior to performing the search.**

- Policy records: any policy directives, guidance documents, memoranda, training materials, or similar records governing the use of face recognition technology for immigration, law enforcement, or other purposes. Any memoranda of understanding between this agency and other agencies to share data, access remote systems or other forms of information sharing with external agencies. **See enclosed SO 5-27**
- Training records: training material governing the use, sharing, or access to any related data related to or collected by the face recognition software/technology, including the legal standard that is required before using the technology. Documents, should they exist, about training for bias in the use of facial recognition technology. **No responsive records.**
- Use and function records: Materials that describe the function of the software considered or in use by this agency, including emails, handouts, PowerPoint presentations, advertisements, or specification documents. – **No responsive records**
- Data: Documents sufficient to describe the source of photos for facial recognition which may include your agency booking photos, other agency booking photos as well as DMV photos. Documents sufficient to show the number of photos in your facial recognition database. Documents that describe the data retention policy of your agency for facial recognition. Documents describing where your agencies use facial recognition technology including at county jails, on body worn cameras, fixed surveillance cameras etc.- **No responsive records**

Respectfully,

A handwritten signature in black ink that reads "Barbara Manuel-Crossman". The signature is written in a cursive, flowing style.

Barbara Manuel-Crossman
Sunshine Law Coordinator

MEMORANDUM OF UNDERSTANDING
BETWEEN
ST. LOUIS FUSION CENTER - TERRORISM EARLY WARNING GROUP
AND
POLICE DIVISION OF THE CITY OF ST. LOUIS
FOR PARTICIPATION IN
[REDACTED] **PROJECT**

I. BACKGROUND

The [REDACTED] is an initiative of the St. Louis Fusion Center to facilitate the responsible [REDACTED] that may reside with the St. Louis area agencies.

The St. Louis Fusion Center is a public safety partnership consisting of law enforcement, fire protection, public health, emergency management and private sector agencies. The St. Louis Fusion Center provides a multijurisdictional / multidisciplinary approach to the collection, analysis and dissemination of critical information. The Fusion Center serves the City of St. Louis and the following seven counties in Missouri and Illinois:

1. Franklin County, Missouri
2. Jefferson County, Missouri
3. St. Charles County, Missouri
4. St. Louis County, Missouri
5. Madison County, Illinois
6. St. Clair County, Illinois
7. Monroe County, Illinois

These eight jurisdictions have been designated by the U.S. Department of Homeland Security (DHS) as the St. Louis Urban Area Security Initiative (UASI) area.

II. CONCEPT

The goal of this project is to [REDACTED] from all contributing agencies that have established this Memorandum of Understanding (MOU) with the St. Louis Fusion Center. Participating agencies will [REDACTED] and will have the capability to [REDACTED]

[REDACTED]

[REDACTED]

The [REDACTED] does not use [REDACTED] to [REDACTED]
[REDACTED] Rather, the [REDACTED]
[REDACTED] may then take [REDACTED]
[REDACTED]

III. PURPOSE

This Memorandum of Understanding (MOU) sets forth an agreement between and defines the roles and responsibilities of the St. Louis Fusion Center (hereinafter referred to as FUSION CENTER) and the Police Division of the City of St. Louis (hereinafter referred to as CONTRIBUTING AGENCY), in implementing [REDACTED] for the purpose of [REDACTED]
[REDACTED]

IV. RESPONSIBILITIES

A. FUSION CENTER

The roles and responsibilities of the FUSION CENTER in this MOU are as follows:

1. The FUSION CENTER will establish [REDACTED]
[REDACTED] to the benefit of all law enforcement agencies in the St. Louis UASI Region.
2. The FUSION CENTER will appoint a project manager to oversee the [REDACTED] and implement the terms and conditions of this MOU.
3. The FUSION CENTER will abide by the Department of Homeland Security (DHS)-approved St. Louis Fusion Center "Privacy, Civil Liberties, and Civil Rights Policy" (P/CLCR) in its management of the [REDACTED] Accountability and enforcement for violations of this policy is explained in section XIII-6 of the P/CLCR Policy.
4. The FUSION CENTER will direct the management of all obligations, responsibilities, and assets of [REDACTED] including but not limited to:
[REDACTED]

a) Any and all contractual obligations for development, implementation, expansion, maintenance, and management of [REDACTED]

b) Ownership of any and all equipment in the inventory of [REDACTED] including but not limited to servers, workstations, communications devices, routers, firewalls or other hardware, and all software in use or under development in compliance with the requirements of [REDACTED]

c) Enrollment, security, access to, and control of any data in the [REDACTED] must meet or exceed standards of the FBI's Criminal Justice Information Services (CJIS) Security Policy.

5. The FUSION CENTER will forward any open record requests and/or subpoenas for [REDACTED] to the CONTRIBUTING AGENCY who will be responsible for responding to the requests or subpoenas.

B. CONTRIBUTING AGENCY

The roles and responsibilities of the CONTRIBUTING AGENCY in this MOU are as follows:

1. The CONTRIBUTING AGENCY agrees to share the following [REDACTED] it has caused [REDACTED] with all law enforcement agencies within the St. Louis UASI region:

a) [REDACTED]

b) [REDACTED]

2. The CONTRIBUTING AGENCY maintains sole authority and responsibility for determining the actions, if any, that are appropriate for the department's information technology environment, and for implementing any changes deemed to be

appropriate to the purposes of this project.

3. The Chief Executive Officer of the CONTRIBUTING AGENCY will review the St. Louis Fusion Center's Privacy, Civil Liberties, and Civil Rights Policy and agrees to remain in compliance with the requirements, policies, and practices as outlined therein for the duration of the CONTRIBUTING AGENCY'S participation in the [REDACTED]
4. The CONTRIBUTING AGENCY will ensure that appropriate personnel are made available as reasonably necessary to assist with development, implementation, and testing of any hardware / software solutions, as well as for any training required, for the purposes of this project.
5. The CONTRIBUTING AGENCY will be responsible for responding to any open record requests and/or subpoenas for [REDACTED]

C. ALL PARTIES

1. The ownership of the data that is housed in this system shall remain with the CONTRIBUTING AGENCY and will not be modified in content by the Fusion Center. Therefore, all ownership rights are to the sole authority and responsibility of the CONTRIBUTING AGENCY. The data in this system is shared by the CONTRIBUTING AGENCY, for the cooperative use by other law enforcement agency personnel. All data use and handling shall comply with the current laws and statutes with respect to the data.
2. Responsibility for responding to liability issues rest with the agency whose employee is accused of and/or admits to the alleged misuse or other misconduct related to the [REDACTED]
3. Administrative discipline responsibilities regarding the misuse or misconduct of [REDACTED] data rest with the agency employing the accused person at the time of the alleged misconduct.

V. FUNDING

Any costs associated with maintenance, upgrade, or changes required directly to the CONTRIBUTING AGENCY'S [REDACTED] system or existing computer network in order to accommodate implementation of the [REDACTED] [REDACTED] interfaces and replication, will be the responsibility [REDACTED]

of the CONTRIBUTING AGENCY. At the time this document was drafted, [REDACTED] system operational costs are to be borne by funding provided through the East-West Gateway Council of Governments and its' St. Louis Area Regional Response System (STARRS) and/or the State of Missouri, and should that funding be depleted or end, contributing agencies will meet to resolve operational cost issues or to suspend operations

VI. TERM OF MOU

- A. This MOU will commence immediately upon signature by both parties.
- B. The CONTRIBUTING AGENCY or the FUSION CENTER may terminate this agreement upon thirty (30) days notice in writing to the other party or, upon mutual agreement, the agreement may be terminated immediately.

FUSION CENTER

NAME
(PRINTED): Michael Besculski
TITLE: Commander
SIGNATURE: Capt Michael Besculski
DATE: 1/27/16

CONTRIBUTING AGENCY

NAME
(PRINTED): D. SAMUEL DOTSON
TITLE: COMMISSIONER OF POLICE
SIGNATURE: D. Samuel Dotson
DATE: 1.12.16.



METROPOLITAN POLICE DEPARTMENT – CITY OF ST. LOUIS
OFFICE OF THE POLICE COMMISSIONER
SPECIAL ORDER

Date Issued: April 19, 2016 **Order No.:** Section V of SO 5-27

Effective Date: April 19, 2016 **Expiration:** Indefinite

Reference:

CALEA Standards:

Cancelled Publications:

Subject: ST. LOUIS MUGSHOT RECOGNITION TECHNOLOGY (SMRT)

To: ALL BUREAUS, DISTRICTS AND DIVISIONS

PURPOSE: To establish guidelines and principles for the collection, analysis, use, dissemination, retention, and destruction of information (also known as data) regarding the St. Louis Mugshot Recognition Technology's (SMRT) operations.

POLICY: SLMPD will comply with all applicable laws and regulations as they pertain to the collection, analysis, use, dissemination, retention, and destruction of data obtained through its St. Louis Mugshot Recognition Technology (SMRT) system. The SLMPD will utilize and share information with the St. Louis Fusion Center (SLFC), [REDACTED] SMRT Database Server [REDACTED]

Redacted per 610.021(21)

A. GENERAL INFORMATION

1. The SMRT Server system, managed by SLFC, provides the database, query tool, history tracking, and reporting for the SMRT program. It manages and provides a temporary storage and search structure for the probe image information being collected in the field. It does not provide analytic search-capable storage of that in-the-field-created information beyond its comparison, as a probe image, to stored mugshots. [REDACTED]
2. The SMRT system does not use facial recognition analysis to positively identify individuals. Rather, the technology applies an algorithm to compile an array of photographs with physical characteristics similar to those of the suspect in the submitted photo. Investigators may then take the logical investigative steps, under proper legal authority, to generate and pursue leads based upon the results.
3. The SMRT Server receives from participating agencies data from mugshot booking observations and organizes the received data in a central database. This central database provides the basis for reporting and query functions. SLFC-authorized personnel will have the ability to:
 - a. Query the image database in the system and view the returned image(s), if any, of matches; and

- b. View basic booking data associated with the returned image(s).

B. USING SMRT

1. Specifically, absent a final court order requiring or authorizing some different use(s), the shared SMRT data may be used for the following purposes (and in any prosecution(s) resulting from such use):
 - a. the investigation, detection, or analysis of crime;
 - b. the investigation, detection, or analysis of violation of Missouri, and/or Illinois, and/or federal criminal or other public safety law;
 - c. the investigation, detection, or analysis of the operation of one or more terrorist(s);
 - d. the investigation, detection, or analysis of missing or endangered person(s); or
 - e. to enable law enforcement personnel to gain accurate identification verification regarding persons encountered in public safety situations, such as traffic stops, pedestrian interviews, vehicle accidents, workplace injuries, and/or assault/shooting scenes; lost/found elderly, mentally-disabled, and/or non-communicative persons; and/or children found with adults not their parents/guardians; and/or in contexts when persons seem to have provided, instead of their true names, entirely-false names, partially-false names, relatives' names, nicknames, purposeful misspellings of true names, and/or names that have been modified without a court order (such as by adding a self-chosen appendage to a surname).
2. The above are non-exclusive examples of legitimate law enforcement uses of the shared SMRT data. In providing this list, this policy is not meant to inhibit other legitimate law enforcement use(s) of the SMRT system for any other purpose(s) for which visual examination of booking mugshots traditionally and lawfully occurs.
3. In no event will access to the SMRT system database be permitted to investigate, analyze, review, or gather information solely concerning any action or speech protected by the First Amendment to the United States Constitution.
4. In no event will any query of the SMRT system database occur other than by a human-initiated query (i.e., automated mass query processes associated with data-mining-type activity will not be permitted).
5. The collection of mugshot images by Project-participating agencies using cameras in any manner known to the collecting agency to solely reflect an individual's political, religious, or social views, associations, or activities (i.e., not as a result of post-arrest booking or any other contact with a law enforcement agency for which mugshot photographs are generally taken) must be limited to instances directly related to criminal conduct or activity which, as standard practice, required an agency to take a mugshot image of a person.

C. SMRT INQUIRIES

1. Detectives or Officers can request the use of SMRT by contacting the Real-Time Crime Center (RTCC).

SO 5-27

2. Detectives or Officers must identify the reason of the request, complaint number, or any other possible identifier or information regarding the request.
3. SMRT requires the highest quality image able to be obtained.
 - a. Large digital images/files may require delivery of a CD, DVD, or other storage device with the image to the RTCC.
 - b. Investigators can also provide information to the RTCC regarding the source from which the image was obtained.
4. The RTCC will generate a Facial Recognition Image Compare Report.



NOTE: Identity comparisons with SMRT are nonscientific and are intended for investigative lead purposes only. These investigative leads should not be used as the sole basis for any decision in the investigation. The intent of this SMRT analysis is only to illustrate facial similarities or differences between two subjects – not to make a positive identification.

5. In the event that the information provided by the RTCC in the Facial Recognition Image Compare Report is used to make a positive identification, the Facial Recognition Image Compare Report will be seized as evidence and handled in accordance with Department policy.
6. Detectives or Officers will fully document the use of any positive identification that was made with the assistance of the SMRT system in the I/Leads report.

D. DATA COLLECTION, RETENTION, AND DISEMINATION

1. SMRT data (i.e., booking mugshots and associated identifying information routinely accompanying mugshots) collected by the law enforcement agencies participating in the SMRT Data Sharing Project will be transmitted to the SLFC-designated SMRT Server, housed at a secure, law enforcement-access-only computer operations center, via a fiber optic line, an encrypted Virtual Private Network (VPN), or a similarly-secure data transmission method.

Redacted per 610.021(21)

2. The data will be maintained on the SMRT server 


3. All SMRT system data provided to the SLFC will be stored on the SMRT server for a period not to exceed ten (10) days after the date that the originating agency for each submitted image notifies the SMRT System Administrator that it no longer retains the mugshot in its records.

4. Should SMRT system data be determined to have evidentiary value, the following applies:
 - a. In those circumstances when data is identified as having evidentiary value, the SMRT System Administrator, or designee, must be notified in writing of that circumstance and, absent receipt of a written retention order from an appropriate authority, will review the facts of the specific case and determine if the data should be saved. If, upon review or upon receipt of a retention order from an appropriate authority, the

SO 5-27

SMRT System Administrator or designee determines it is reasonable to believe the data has evidentiary value, the SMRT System Administrator or designee will authorize the transfer of the applicable data from the SMRT Program server to a form of digital storage media (CD, DVD, etc.) or other portable storage devices.

- b. Agencies requiring data to be retained by the SLFC beyond the established retention period may make a formal request to the SLFC to extend retention. Each request must specify the need for extended retention, the circumstances surrounding the request, the requesting agency's case number, and a specific point of contact within the requesting agency. The SLFC may grant or deny agency requests based on the information provided and applicable law.

E. AUDIT LOGS

1. All transactions and queries of the SMRT Server system are logged, immutably, and are subject to review at any time. Anyone found to misuse the system is subject to disciplinary action, up to and including criminal prosecution.
2. In order to facilitate the periodic and random audits necessary to monitor user compliance with laws and policies, audit logs will include certain information. Specifically, queries to the SMRT Server will be immutably logged and include:
 - a. The identity and purpose of the user initiating the query;
 - b. The probe image element used to query the SMRT system (however, the probe image will not be enrolled in the system for future searches, but is retained only as an audit-enabling feature);
 - c. Valid reason for the search; and
 - d. Date and time of the inquiry.

F. RESPONSIBILITIES

1. Primary responsibility for ensuring compliance with the provisions of this policy is assigned to the Commander of the RTCC.
2. The Commander of the Real-Time Crime Center will designate an SMRT System Administrator, who will be responsible for the overall management of the SMRT Program.
3. Both the Commander of the RTCC and the SMRT System Administrator will be responsible for making SMRT system reports available to the public, as well as for ensuring that this SO document is both available to the public and, as may be needed, is updated.